(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
12. Juni 2003 (12.06.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/049365 A1

(51) Internationale Patentklassifikation[7]: H04L 9/32, 29/06, H04Q 7/38

(21) Internationales Aktenzeichen: PCT/DE01/04461

(22) Internationales Anmeldedatum:
29. November 2001 (29.11.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **CUELLAR, Jorge** [DE/DE]; Höllriegelskreuther Weg, 82065 Baierbrunn (DE). **MARHOEFER, Michael** [DE/DE]; Wendelsteinstrasse 6, 82041 Deisenhofen (DE).

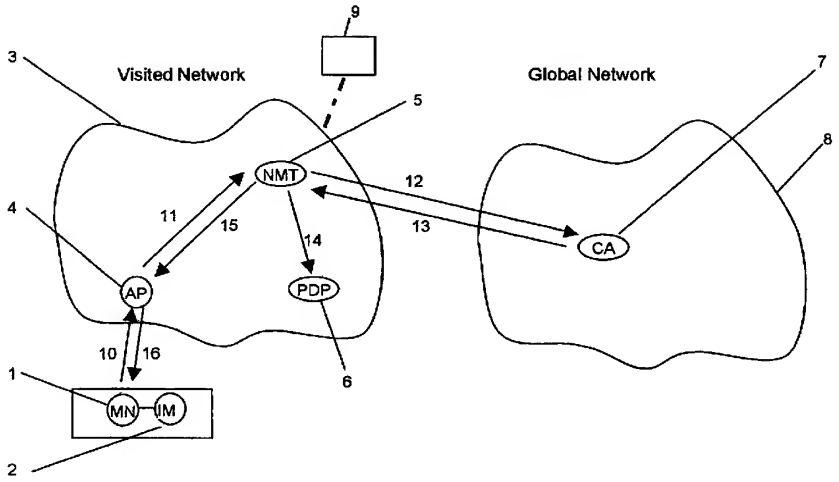
(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Fortsetzung auf der nächsten Seite]

(54) **Title:** USE OF A PUBLIC KEY KEY PAIR IN THE TERMINAL FOR AUTHENTICATION AND AUTHORISATION OF THE TELECOMMUNICATION USER WITH THE NETWORK OPERATOR AND BUSINESS PARTNERS

(54) **Bezeichnung:** NUTZUNG EINES PUBLIC-KEY-SCHLÜSSELPAARES IM ENDGERÄT ZUR AUTHENTISIERUNG UND AUTORISIERUNG DES TELEKOMMUNIKATIONS-TEILNEHMERS GEGENÜBER DEM NETZBETREIBER UND GESCHÄFTSPARTNERN



(57) **Abstract:** A very efficient authentication and authorisation check in n: m relationships is possible with a method for checking the entitlement of a user of a telecommunication terminal (1) to a service, whereby an access device (4) on a telecommunication network (3) obtains at least one certificate and a proof of identity (10) from the telecommunication terminal (1), whereupon NMT (5) together with a certification device (7) carries out a check of whether the certificate giving the identity is valid and has a positive status and whether particular authorisation may be obtained from complementary certificates. Should the above be the case, a secret (for example a session key) is transmitted (15) to the access device (4) which is also sent (15, 16) to the telecommunication terminal (1, 2), encoded with at least the public key. The access device (4) is then activated with a policy corresponding to the rights of the telecommunication user.

[Fortsetzung auf der nächsten Seite]

WO 03/049365 A1

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Eine sehr effizeinte Authentisierungs- und Autorisierungs-Prüfung in n: m-Verhältnissen wird ermöglicht durch ein Verfahren zur Prüfung der Berechtigung eines Nutzers eines Telekommunikationsendgerätes (1) für einen Dienst, wobei eine Zugangseinrichtung (4) eines Telekommunikationsendgerätes (1) für einen Dienst, wobei eine Zugangseinrichtung (4) eines Telekommunikations-netzes (3) vom Telekommunikationsendgerät (1) zumindest ein Zertifikat und einen Identitätsnachweis erhält (10), wonach NMT (5) zusammen mit einer Zertifizierungseinrichtung (7) eine Prüfung dahingehend durchführt, ob das identitäts-bestätigende Zertifikat gültig ist und einen positiven Status hat und ob sich aus ergänzenden Zertifikaten besondere Berechtigungen ergebenk wobei, falls dies der Fall ist, der Zugangseinrichtung (4) ein Geheimis (z.B. session key) übersandt (15) wird, das mit zumindest dem öffentlichen Schlüssel verschlüsselt auch an das Telekommunikationsendgerät (1, 2) gesand (15, 16) wird und die Zugangseinrichtung (4) mittels einer den Rechten des Telekommunikationsteilnehmers entsprechenden Policy freigeschaltet wird.

Beschreibung

Titel „Nutzung eines Public-Key-Schlüsselpaares im Endgerät zur Authentisierung und Autorisierung des Telekommunikationsteilnehmers gegenüber dem Netzbetreiber und Geschäftspartnern"

Die Erfindung betrifft Vorrichtungen und Verfahren zum Prüfen der Berechtigung (Authentisierung und/oder Autorisierung) eines Teilnehmers gegenüber einer Zugangseinrichtung eines Telekommunikationsnetzes oder gegenüber einem über dieses Netz erreichbaren weiteren Diensteanbieter.

Gemäß z.B. dem GSM-Standard verwendet eine GSM-Mobilstation (Handy) eine SIM-Karte eines Teilnehmers, die ein die SIM-Karte identifizierendes Geheimnis enthält, dass auch dem Netzbetreiber bekannt ist (Shared Secret) sowie eine vom die Mobilfunkstation benutzenden Teilnehmer abgefragte PIN-Nummer. Durch ein geeignetes Protokoll (z.B. das Challenge-Response-Protokoll zur GSM-Authentisierung) kann ein Netzbetreiber eine SIM-Karte eines Benutzers identifizieren und dem Teilnehmer beispielsweise die Benutzung des Mobilfunknetzes gestatten oder verweigern. Dieses Verfahren eignet sich jedoch nur zur Authentisierung in n:1-Beziehungen (Authentisierung von zum Beispiel n potentiellen Teilnehmern eines Mobilfunknetzes gegenüber einem Netzbetreiber), ist jedoch ungeeignet, um den Benutzer auch gegenüber mehreren potentiellen (im Voraus nicht abschließend bekannten) Geschäftspartnern (n: m-Beziehung) zu authentisieren.

Aufgabe der vorliegenden Erfindung ist es deshalb, eine einfache und effiziente Authentisierung und Autorisierung eines Telekommunikationsteilnehmers für bestimmte Dienste oder Transaktionen über ein Telekommunikationsnetz gegenüber einer Zugangseinrichtung eines Telekommunikationsnetzes, welches der Telekommunikationsteilnehmer über ein Telekommunikationsendgerät mit einem Telekommunikationsteilnehmeridentitätsmo-

dul benutzen möchte, zu ermöglichen. Die Aufgabe wird jeweils durch die Gegenstände der unabhängigen Ansprüche gelöst.

Die Erfindung erlaubt eine einfache und effiziente Authentisierung eines Telekommunikationsteilnehmers gegenüber dem Telekommunikationsnetz, über welches er (zur Abwicklung der Dienste wie Transaktionen etc.) kommuniziert und auch eine einfache und effiziente Authentiserung und/oder Autorisierung gegenüber Dritten für vorgegebene Dienste wie Transaktionen (vertrauliche E-Mail, Bankgeschäfte, Bezahlungen etc.).

Das erfindungsgemäße Verfahren funktioniert auch bei n: m-Beziehungen wie der Authentisierung von potentiellen Telekommunikationsteilnehmern durch Telekommunikationsteilnehmeridentitätsmodule in Telekommunikationsendgeräten gegenüber mehreren (m) Connectivity-Providern für peer-to-peer-Transaktionen zwischen Endanwendern, in Adhoc-Networken etc. erlaubt die Generierung eines Zusatznutzens (für rechtliche Verbindlichkeit von Bestellungen, Überweisungen, etc.) bei der Verwendung von Public-key Schlüsselpaaren, erlaubt die Mehrfachnutzung vorhandener Komponenten (Telekommunikationsteilnehmeridentitätsmodule) ohne Erhöhung Endgeräte-seitiger Hardware-Kosten und schafft einen sehr hohen Grad an Sicherheit.

Das Verfahren ist insbesondere dazu geeignet, mobile Endgeräte gegenüber einem Internetprotokoll-Netz für die Nutzung dieses Netzes selbst sowie für Dienste, welche Dritte über das Internetprotokoll-Netz anbieten zu authentisieren.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus den Unteransprüchen und der nachfolgenden Beschreibung eines Ausführungsbeispieles anhand der Zeichnung. Dabei zeigt:

Fig. 1 schematisch eine erfindungsgemäße Berechtigungsprüfung

Figur 1 zeigt ein Telekommunikationsendgerät 1 (mobile node MN, z.B. zellulares Mobilfunkendgerät für GSM, UMTS etc.) mit einem damit verbundenen (beispielsweise darin einfügbaren) Telekommunikationsteilnehmeridentitätsmodul 2 (z.B. SIM, W-SIM, UICC eines U-SIM etc.), ein besuchtes Telekommunikationsnetz 3 (beispielsweise ein Internetprotokoll-Netz eines Mobiltelekommunikationsnetzes etc.) mit einer Zugangseinrichtung 4 (AP = Access Point) zum Telekommunikationsnetz 3, mit einer Netzwerkmanagementeinrichtung 5 (NMT = Network Management Tool) und einer Zugangsverwaltungsinstanz 6 (PDP = Policy Decision Point). Vom Telekommunikationsnetz 3, welches der Benutzer des Telekommunikationsendgerätes 1 nutzen möchte, kann eine Zertifizierungseinrichtung 7, die auch ein öffentlich zugängliches Verzeichnis der von ihr generierten Zertifikate sowie der diesen Zertifikaten zugeordneten Statusangaben anbietet (im gleichen Telekommunikationsnetz 3 oder in einem anderen Telekommunikationsnetz 8 oder bei einem anderen Betreiber oder in einem Trust-Center, auf welches von Elementen des Telekommunikationsnetzes 3 zugegriffen werden kann), kontaktiert werden zur Überprüfung von im Telekommunikationsendgerät 1 gespeicherten Identitätsangaben (MSISDN etc), Zertifikaten und zur Abfrage der zugehörigen Statusdaten des Telekommunikationsteilnehmers 1 betreffend die Durchführung von Diensten. Diese Dienste umfassen z.B. Transportdienste, insbesondere die Nutzung des Telekommunikationsnetzes 3 selbst, und/oder Anwendungsdienste wie beispielsweise ortsbezogene Dienste und/ oder Transaktionen wie beispielsweise Bestellungen, Überweisungen etc. mit Anbieter 9 über das Telekommunikationsnetz 3.

Der Benutzer des Telekommunikationsendgerätes 1 möchte gegenüber dem Betreiber des Netzwerkes 3 und / oder einem Anbieter 9 (innerhalb des Telekommunikationsnetzes 3 oder außerhalb des Telekommunikationsnetzes 3, beispielsweise auch ein vom Telekommunikationsnetz unabhängiger dritter Anbieter, welcher seine Dienste nur über das Telekommunikationsnetz 3 anbietet), seine Berechtigung zur Inanspruchnahme von Diensten des

Anbieters von 3 oder 9 nachweisen, also eine Authentisierung und/oder Autorisierung durchführen. Die Authentisierung und/oder Autorisierung erfolgt gegenüber dem Telekommunikationsnetz 3 oder dem Anbieter des Dienstes 9 (z.B. von dem NMT (5)), sobald die Identitätsangabe (MSISDN etc) und die Berechtigung des Telekommunikationsteilnehmers 1 (bzw. des Telekommunikationsteilnehmeridentitätsmoduls 2) überprüft wurde.

Die Überprüfung der Identitätsangabe und Berechtigung des Telekommunikationsteilnehmers 1 erfolgt hier durch Überprüfung eines oder mehrerer in dessen Telekommunikationsteilnehmeridentitätsmodul 2 gespeicherten Zertifikate(s) sowie unter Anwendung eines ebenfalls im Teilnehmeridentitätsmodul 2 gespeicherten privaten Schlüssels eines asymmetrischen (PKI-basierten) Schlüsselpaares. Die Überprüfung wird beispielsweise bei dem Versuch einer Einbuchung des Telekommunikationsteilnehmerendgerätes 1 in das Telekommunikationsnetz 3 im Rahmen eines Autorisierungsüberprüfungsverfahrens zwischen der NMT, Zugangseinrichtung AP 4 und dem Telekommunikationsteilnehmerendgerät 1 durch Überprüfung des Zertifikates / der Zertifikate und Abfrage der zugeordneten Statusdaten in der Zertifizierungseinrichtung 7 durchgeführt. Der NMT verifiziert die Gültigkeit des Zertifikates durch eine OCSP- oder CRL- Abfrage bei CA 7.

Das Telekommunikationsteilnehmeridentitätsmodul 1 übersendet, wenn es sich gegenüber der Zugangseinrichtung 4 autorisieren möchte, nach Eingabe einer PIN oder einer sonstigen für den Telekommunikationsteilnehmer spezifischen Eingabe (Fingerabdruck etc), der Zugangseinrichtung 4 (beispielsweise auf ein Angebot (Challenge) der Zugangseinrichtung 4 unter Übermittlung einer Challenge-Nummer hin) eine Identitätsangabe (betreffend die Identität des Telekommunikationsteilnehmeridentitätsmoduls oder des Endgerätes und/oder des Benutzers), ein oder mehrere (aus einer Identitäts- und/oder zugeordneten Berechtigungsangabe, einem öffentlichen Schlüssel eines asymmetrischen Schlüsselpaares mit einem durch nur der Zertifi-

zierungseinrichtung 7 bekannten Zertifikatgenerierungsverfahren generierbares) Zertifikat, sowie einen durch den privaten Schlüssel aus dem Telekommunikationsteilnehmeridentitätsmodul signierten Schutz gegen eine missbräuchliche Wiederholung einer abgefangenen Anfrage durch einen Dritten (replay-protection, nonce). Die Zugangsstelle (AP, 4) übermittelt nach Überprüfung der korrekten Zusendung (z.B. challenge hinreichend frisch, nonce korrekt und mittels des im Teilnehmeridentitätsmodul gespeicherten privaten Schlüssels signiert), das/die Zertifikat(e) an eine für einen Teil des Netzwerkes 3 oder das ganze Netzwerk 3 zuständige Netzwerkmanagementeinrichtung 5 (NMT = Network Management Tool) im Schritt 11.

Die Netzwerkmanagementeinrichtung 5 übersendet das/die Zertifikat(e) im Schritt 12 an eine Zertifizierungseinrichtung 7 (CA = Certification Authority), welche z.B. mittels eines OCSP-Responders und unter Verwendung einer Liste widerrufener Zertifikate (certificate revocation list, CRL) die Gültigkeit des/der Zertifikate(s) und die Korrektheit der angegebenen Identitätsangaben und ggf. Berechtigungen) überprüft und Auskunft gibt über den Status (z.B. gültig/ungültig etc) des/der Zertifikate sowie ggf. die Berechtigungen des Telekommunikationsteilnehmers. Das Zertifikat bestätigt die Identitätsangabe, wenn die Zertifizierungseinrichtung mittels eines ihr bekannten Verfahrens aus dem Zertifikat die Identitätsangabe generieren kann.
Falls aus dem/den Zertifikat(en) von der Zertifizierungseinrichtung 7 der öffentliche Schlüssel und die Identität/Berechtigungen des Telekommunikationsteilnehmers 1,2 und/oder des Mobilfunkendgerätes gewonnen werden kann, und die Statusauskunft (Zertifikat nicht abgelaufen, nicht widerrufen, Berechtigungen etc) ermittelt werden kann, wird der Status des Zertifikates von der Zertifizierungseinrichtung 7 der Netzwerkmanagementeinrichtung 5 im Netzwerk 3 mitgeteilt (13). Die Netzwerkmanagementeinrichtung 5 entscheidet anhand der mitgeteilten Statusangaben und Berechtigungen über den Umfang der Berechtigungen des MN 1, Dienste und Ressourcen

des Telekommunikationsnetzes 3 in Anspruch zu nehmen und teilt dies im Schritt 14 der Zugangsverwaltungsinstanz PDP 6 mit. Entsprechend dieser Entscheidung gibt dann PDP 6 durch Übertragung einer entsprechenden Policy an den AP 4 für den Telekommunikationsteilnehmer 1 die Nutzung des Telekommunikationsnetzes 3 frei oder sie bleibt bei vollständig negativer Entscheidung des NMT 5 weiterhin gesperrt.

Die Netzwerkmanagementeinrichtung 5 kann zentral für das Netzwerk 3 auf Anfrage Dritter 9 mitteilen, ob und für welche Dienste etc. ein Mobilfunkendgerät (1) aktuell von der Zertifizierungseinrichtung 7 als berechtigt betrachtet wird. Ferner wird bei positivem Zertifikatsstatus (Zertifikat gültig etc) ein vom NMT (5) erzeugtes Geheimnis (z.B. session key) mit einem im Netzwerk 3 verwendeten Verschlüsselungsverfahren an die Zugangseinrichtung 4 gesendet und dort entschlüsselt. Ferner wird das gleiche Geheimnis von der Netzwerkmanagementeinrichtung 5 mit dem öffentlichen Schlüssel des Telekommunikationsidentitätsmoduls 2 (welchen öffentlichen Schlüssel die Netzwerkmanagementeinrichtung beim Beginn der Einbuchung vom Endgerät 1 über die Zugangseinrichtung 4 im Schritt 10 erhalten kann) verschlüsselt. Weiterhin kann das NMT 5 sein eigenes Zertifikat über den AP 4 an den NM 1 übertragen.
Hierauf wird von der Zugangseinrichtung 4 mit dem ihr bekannten (im Telekommunikationsnetz vorgesehenen) Schlüssel das Geheimnis entschlüsselt und darauf wird im Schritt 16 das immer noch mit dem öffentlichen Schlüssel des Telekommunikationsteilnehmeridentitätsmoduls 2 verschlüsselte Geheimnis an das Telekommunikationsteilnehmeridentitätsmodul 2 übertragen. Im Telekommunikationsteilnehmeridentitätsmodul 2 ist auch der zum genannten öffentlichen Schlüssel zugehörige private Schlüssel gespeichert und wird gewendet um das Geheimnis zu entschlüsseln. Daraufhin kann dieses Geheimnis beispielsweise zur vertraulichen Kommunikation zwischen dem Endgerät 1 und der Zugangseinrichtung 4 verwendet werden.
Die Zugangseinrichtung (4) nimmt den Teilnehmer in eine Liste von Telekommunikationsteilnehmern mit Zugang zum Telekommuni-

kationsnetz (3) und/ oder Dienst (9) auf, und gewährt den Zugang zum Telekommunikationsnetz und/ oder Dienst (9) nur in die Liste aufgenommenen Teilnehmern.

Weiterhin kann ein Telekommunikationsendgerät 1 mit dem Telekommunikationsteilnehmeridentitätsmodul 2 bei einem Dritten (9) beispielsweise (je nach dem was das/die Zertifikat zulässt/zulassen) weitere Dienste und Ressourcen in Anspruch nehmen, Waren bestellen, elektronisch bezahlen etc., wobei der Dritte (9) entweder bei einer Einrichtung NMT 5 des Telekommunikationsnetzes 3 sich den Grad der Berechtigungen bestätigen lässt oder bei der CA 7 (s.o.) nachfragt.

Patentansprüche

1. Verfahren zur Prüfung der Berechtigung eines Teilnehmers eines Telekommunikationsendgerätes (1) zur Inanspruchnahme eines Dienstes (9) und/ oder Benutzung eines Telekommunikationsnetzes,
wobei eine Zugangseinrichtung (4) eines Telekommunikationsnetzes (3) vom Telekommunikationsendgerät (1) zumindest ein Zertifikat und eine Identitätsangabe erhält (10),
wonach eine Netzwerkmanagementeinrichtung (NMT 5) oder eine Zertifizierungseinrichtung (7) eine Prüfung dahingehend durchführt, ob das Zertifikat die Identitätsangabe bestätigt und einen positiven Status hat,
wobei, falls dies der Fall ist, der Zugangseinrichtung (4) ein Geheimnis (session key 15) übersandt wird, das mit zumindest dem öffentlichen Schlüssel verschlüsselt auch an das Telekommunikationsendgerät (1, 2) gesandt (15, 16) wird.

2. Verfahren nach Anspruch 1
d a d u r c h g e k e n n z e i c h n e t,
dass nach der Übersendung des Geheimnisses die Zugangseinrichtung (4) den Teilnehmer in eine Liste von Telekommunikationsteilnehmern mit Zugang zum Telekommunikationsnetz (3) und/oder Dienst (9) aufnimmt,
wobei die Zugangseinrichtung (4) den Zugang zum Telekommunikationsnetz (3) und/ oder zum Dienst (9) nur in die Liste aufgenommenen Teilnehmern gewährt.

3. Verfahren nach Anspruch 1 oder 2,
d a d u r c h g e k e n n z e i c h n e t,
dass die Zugangseinrichtung (4) das vom Telekommunikationsendgerät (1) erhaltene Zertifikat, die Identität und eine replay- protection an eine Netzwerkmanagementeinrichtung (5) des Telekommunikationsnetzes (3) sendet,
welche von der Zertifizierungseinrichtung (7) die Prüfung

durchführen lässt und bei positiver Prüfung das Geheimnis an die Zugangseinrichtung (4) und über die Zugangseinrichtung (4) an das Telekommunikationsendgerät (1) sendet (15,16).

4. Verfahren nach einem der vorhergehenden Ansprüche d a d u r c h g e k e n n z e i c h n e t, dass das Ergebnis der Prüfung der Zertifizierungseinrichtung (7) von der Netzwerkmanagementeinrichtung (5) an eine Dienstverwaltungseinrichtung (6) mitgeteilt wird.

5. Verfahren nach einem der vorhergehenden Ansprüche d a d u r c h g e k e n n z e i c h n e t, dass die Zertifizierungsinstanz (7) in einem anderen Netzwerk angeordnet ist als die Zugangseinrichtung (4).

6. Verfahren nach einem der vorhergehenden Ansprüche 1 bis 4 d a d u r c h g e k e n n z e i c h n e t, dass die Zertifizierungseinrichtung (7) im gleichen Telekommunikationsnetz angeordnet ist wie die Zugangseinrichtung (4).

7. Verfahren nach einem der vorhergehenden Ansprüche d a d u r c h g e k e n n z e i c h n e t, dass der private Schlüssel des Schlüsselpaares nur in einem Telekommunikationsteilnehmeridentitätsmodul (2) des Telekommunikationsendgerätes (1) gespeichert ist.

8. Verfahren nach einem der vorhergehenden Ansprüche d a d u r c h g e k e n n z e i c h n e t, dass das Telekommunikationsnetz ein Internet-Protokoll-Netz ist.

9. Verfahren nach einem der vorhergehenden Ansprüche d a d u r c h g e k e n n z e i c h n e t, dass das Telekommunikationsnetz ein zellulares Mobilfunknetz ist.

10. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t,
dass für ein Telekommunikationsteilnehmeridentitätsmodul mehrere Zertifikate, insb. Attributzertifikate verwendbar sind, deren positive Prüfung jeweils das Telekommunikationsendgerät für zumindest eine Art von Transaktionen oder sonstigen Diensten oder Berechtigungen zulässt.

11. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t,
dass bei positiver Prüfung (7) dem Telekommunikationsendgerät die Benutzung von durch Dritten (9) über das Telekommunikationsnetz (3) angebotenen Transaktionen oder Diensten ermöglicht wird.

12. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t,
dass das Telekommunikationsteilnehmeridentitätsmodul (2) einen zum öffentlichen Schlüssel passenden privaten Schlüssel gespeichert hat und zur Entschlüsselung des mit dem öffentlichen Schlüssel verschlüsselten Geheimnisses verwendet.

13. Telekommunikationsnetz, insbesondere zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche,
mit
- einer Zugangseinrichtung (4) zum Empfang eines von einem Telekommunikationsendgerät (1) übersandten (10) Zertifikates und Identitätsangabe,
- einem Zugang zu einer Zertifizierungseinrichtung (7) mit einem Zertifikatgenerierungsverfahren zum Generieren von Zertifikaten aus öffentlichen Schlüsseln, welche Zertifizierungseinrichtung die Gültigkeit eines Zertifikates sowie zugehörige Statusangaben auf Anfrage mitteilt (13),
wobei der Zugang eines Telekommunikationsendgerätes (1) zu einem für Inhaber (1) eines Zertifikates erlaubten

Dienst eines Anbieters (9) durch eine Einrichtung (4;6) des Telekommunikationsnetzes (3) nur insoweit gewährt wird, wie die Prüfung eines Zertifikates / der Zertifikate des Telekommunikationsendgerätes durch die Zertifizierungseinrichtung (7) anhand des öffentlichen Schlüssels erfolgreich war.

14. Telekommunikationsteilnehmeridentitätsmodul (2), insbesondere zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 12,
mit einem Speicher für mindestens einen privaten und öffentlichen Schlüssel eines Schlüsselpaares und für ein Zertifikat, welche zusammen zur Berechtigungsprüfung für Dienste (9) eines Telekommunikationsnetzes vorgesehen sind.

2001E06926DE

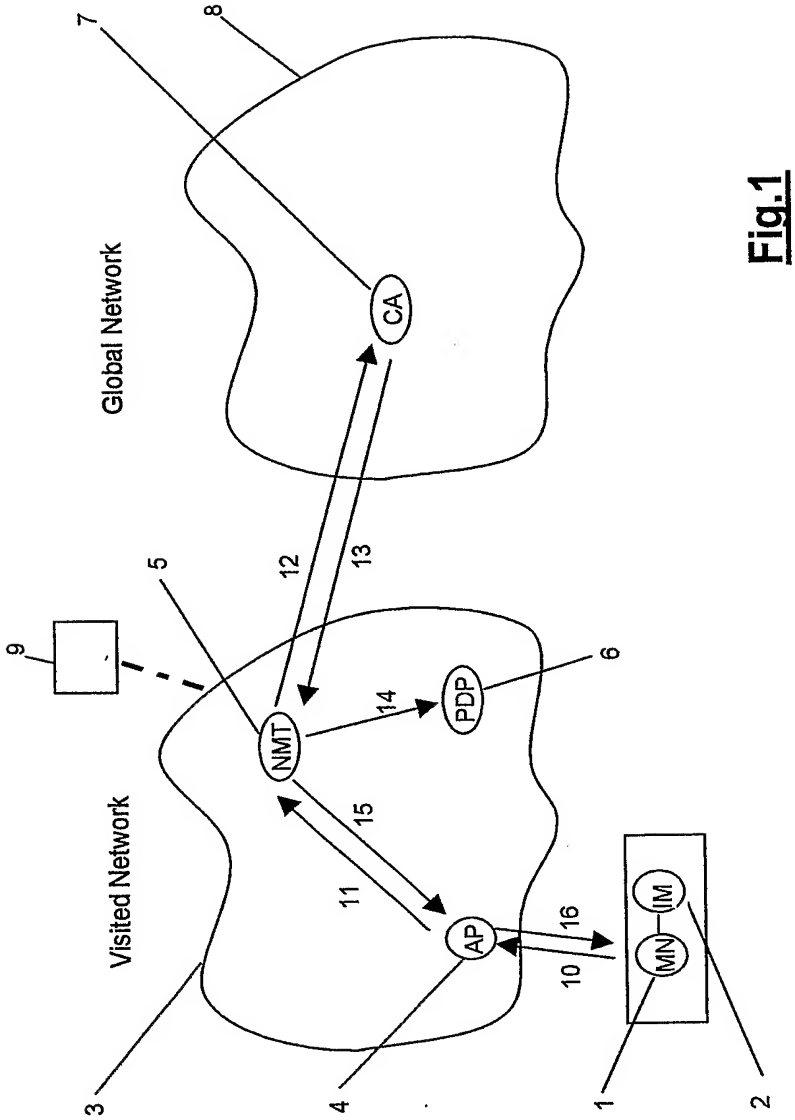


Fig.1

INTERNATIONAL SEARCH REPORT

Inter ıal Application No
PCT/DE 01/04461

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 H04L29/06 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, COMPENDEX, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 903 887 A (AT & T CORP) 24 March 1999 (1999-03-24)	1-13
X	column 2, paragraph 7 - paragraph 8 ---	14
A	PUTZ S ET AL: "Authentication schemes for third generation mobile radio systems" PERSONAL, INDOOR AND MOBILE RADIO COMMUNICATIONS, 1998. THE NINTH IEEE INTERNATIONAL SYMPOSIUM ON BOSTON, MA, USA 8-11 SEPT. 1998, NEW YORK, NY, USA,IEEE, US, 8 September 1998 (1998-09-08), pages 126-130, XP010314761 ISBN: 0-7803-4872-9 page 127, right-hand column, last paragraph -page 128, right-hand column, paragraph 1 --- -/--	1-14

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 August 2002	09/08/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Huber, O

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/DE 01/04461

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01 02940 A (LAPSTUN JACQUELINE ANNE ;SILVERBROOK RES PTY LTD (AU); LAPSTUN PAU) 11 January 2001 (2001-01-11) page 31, line 27 -page 32, line 20	1,13,14
A	PARK CH-S: "ON CERTIFICATE-BASED SECURITY PROTOCOLS FOR WIRELESS MOBILE COMMUNICATION SYSTEMS" IEEE NETWORK, IEEE INC. NEW YORK, US, vol. 11, no. 5, 1 September 1997 (1997-09-01), pages 50-55, XP000699941 ISSN: 0890-8044 page 52, right-hand column, paragraph 2 -page 54, left-hand column, paragraph 1	1-14

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

rmation on patent family members

Interr al Application No
PCT/DE 01/04461

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0903887 A	24-03-1999	US 5204902 A	20-04-1993
		EP 0903887 A2	24-03-1999
		DE 69230330 D1	30-12-1999
		DE 69230330 T2	03-08-2000
		EP 0532227 A2	17-03-1993
		FI 924093 A	14-03-1993
		JP 2589030 B2	12-03-1997
		JP 6188828 A	08-07-1994
WO 0102940 A	11-01-2001	WO 0072241 A1	30-11-2000
		WO 0072242 A1	30-11-2000
		WO 0072202 A1	30-11-2000
		WO 0072232 A1	30-11-2000
		WO 0072233 A1	30-11-2000
		WO 0072234 A1	30-11-2000
		WO 0072235 A1	30-11-2000
		WO 0072138 A1	30-11-2000
		WO 0072124 A1	30-11-2000
		WO 0072192 A1	30-11-2000
		WO 0072243 A1	30-11-2000
		WO 0072236 A1	30-11-2000
		WO 0072244 A1	30-11-2000
		WO 0072576 A1	30-11-2000
		WO 0072237 A1	30-11-2000
		WO 0072125 A1	30-11-2000
		WO 0072247 A1	30-11-2000
		WO 0071353 A1	30-11-2000
		WO 0072248 A1	30-11-2000
		WO 0072245 A1	30-11-2000
		WO 0072203 A1	30-11-2000
		WO 0072204 A1	30-11-2000
		WO 0072499 A1	30-11-2000
		WO 0072505 A1	30-11-2000
		WO 0072136 A1	30-11-2000
		WO 0072503 A1	30-11-2000
		WO 0071355 A1	30-11-2000
		WO 0071356 A1	30-11-2000
		WO 0071354 A1	30-11-2000
		WO 0071362 A1	30-11-2000
		WO 0071357 A1	30-11-2000
		WO 0071455 A1	30-11-2000
		WO 0071348 A1	30-11-2000
		WO 0071350 A1	30-11-2000
		WO 0072137 A1	30-11-2000
		WO 0072126 A1	30-11-2000
		WO 0072127 A1	30-11-2000
		WO 0072286 A1	30-11-2000
		WO 0072128 A1	30-11-2000
		WO 0072129 A1	30-11-2000
		WO 0072230 A1	30-11-2000
		WO 0072238 A1	30-11-2000
		WO 0072287 A1	30-11-2000
		WO 0072249 A1	30-11-2000
		WO 0072130 A1	30-11-2000
		WO 0072250 A1	30-11-2000
		WO 0072110 A2	30-11-2000
		WO 0072131 A1	30-11-2000
		WO 0072132 A1	30-11-2000

INTERNATIONAL SEARCH REPORT

rmation on patent family members

Interr al Application No
PCT/DE 01/04461

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0102940 A		WO 0072133 A1	30-11-2000

INTERNATIONALER RECHERCHENBERICHT

Intern ales Aktenzeichen
PCT/DE 01/04461

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/32 H04L29/06 H04Q7/38

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, INSPEC, COMPENDEX, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A X	EP 0 903 887 A (AT & T CORP) 24. März 1999 (1999-03-24) Spalte 2, Absatz 7 - Absatz 8 ---	1-13 14
A	PUTZ S ET AL: "Authentication schemes for third generation mobile radio systems" PERSONAL, INDOOR AND MOBILE RADIO COMMUNICATIONS, 1998. THE NINTH IEEE INTERNATIONAL SYMPOSIUM ON BOSTON, MA, USA 8-11 SEPT. 1998, NEW YORK, NY, USA,IEEE, US, 8. September 1998 (1998-09-08), Seiten 126-130, XP010314761 ISBN: 0-7803-4872-9 Seite 127, rechte Spalte, letzter Absatz -Seite 128, rechte Spalte, Absatz 1 --- -/--	1-14

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
1. August 2002	09/08/2002

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Huber, O

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 01 02940 A (LAPSTUN JACQUELINE ANNE ;SILVERBROOK RES PTY LTD (AU); LAPSTUN PAU) 11. Januar 2001 (2001-01-11) Seite 31, Zeile 27 -Seite 32, Zeile 20 ---	1,13,14
A	PARK CH-S: "ON CERTIFICATE-BASED SECURITY PROTOCOLS FOR WIRELESS MOBILE COMMUNICATION SYSTEMS" IEEE NETWORK, IEEE INC. NEW YORK, US, Bd. 11, Nr. 5, 1. September 1997 (1997-09-01), Seiten 50-55, XP000699941 ISSN: 0890-8044 Seite 52, rechte Spalte, Absatz 2 -Seite 54, linke Spalte, Absatz 1 -----	1-14

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichun e zur selben Patentfamilie gehoren

Interna les Aktenzeichen
PCT/DE 01/04461

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0903887 A	24-03-1999	US 5204902 A	20-04-1993
		EP 0903887 A2	24-03-1999
		DE 69230330 D1	30-12-1999
		DE 69230330 T2	03-08-2000
		EP 0532227 A2	17-03-1993
		FI 924093 A	14-03-1993
		JP 2589030 B2	12-03-1997
		JP 6188828 A	08-07-1994
WO 0102940 A	11-01-2001	WO 0072241 A1	30-11-2000
		WO 0072242 A1	30-11-2000
		WO 0072202 A1	30-11-2000
		WO 0072232 A1	30-11-2000
		WO 0072233 A1	30-11-2000
		WO 0072234 A1	30-11-2000
		WO 0072235 A1	30-11-2000
		WO 0072138 A1	30-11-2000
		WO 0072124 A1	30-11-2000
		WO 0072192 A1	30-11-2000
		WO 0072243 A1	30-11-2000
		WO 0072236 A1	30-11-2000
		WO 0072244 A1	30-11-2000
		WO 0072576 A1	30-11-2000
		WO 0072237 A1	30-11-2000
		WO 0072125 A1	30-11-2000
		WO 0072247 A1	30-11-2000
		WO 0071353 A1	30-11-2000
		WO 0072248 A1	30-11-2000
		WO 0072245 A1	30-11-2000
		WO 0072203 A1	30-11-2000
		WO 0072204 A1	30-11-2000
		WO 0072499 A1	30-11-2000
		WO 0072505 A1	30-11-2000
		WO 0072136 A1	30-11-2000
		WO 0072503 A1	30-11-2000
		WO 0071355 A1	30-11-2000
		WO 0071356 A1	30-11-2000
		WO 0071354 A1	30-11-2000
		WO 0071362 A1	30-11-2000
		WO 0071357 A1	30-11-2000
		WO 0071455 A1	30-11-2000
		WO 0071348 A1	30-11-2000
		WO 0071350 A1	30-11-2000
		WO 0072137 A1	30-11-2000
		WO 0072126 A1	30-11-2000
		WO 0072127 A1	30-11-2000
		WO 0072286 A1	30-11-2000
		WO 0072128 A1	30-11-2000
		WO 0072129 A1	30-11-2000
		WO 0072230 A1	30-11-2000
		WO 0072238 A1	30-11-2000
		WO 0072287 A1	30-11-2000
		WO 0072249 A1	30-11-2000
		WO 0072130 A1	30-11-2000
		WO 0072250 A1	30-11-2000
		WO 0072110 A2	30-11-2000
		WO 0072131 A1	30-11-2000
		WO 0072132 A1	30-11-2000

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichung..., ...e zur selben Patentfamilie gehören

Interna es Aktenzeichen
PCT/DE 01/04461

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 0102940 A		WO 0072133 A1	30-11-2000

PUB-NO: WO003049365A1

DOCUMENT-IDENTIFIER: WO 3049365 A1

TITLE: USE OF A PUBLIC KEY KEY PAIR IN THE TERMINAL FOR AUTHENTICATION AND AUTHORISATION OF THE TELECOMMUNICATION USER WITH THE NETWORK OPERATOR AND BUSINESS PARTNERS

PUBN-DATE: June 12, 2003

INVENTOR-INFORMATION:

NAME	COUNTRY
CUELLAR, JORGE	DE
MARHOEFER, MICHAEL	DE

ASSIGNEE-INFORMATION:

NAME	COUNTRY
SIEMENS AG	DE
CUELLAR JORGE	DE
MARHOEFER MICHAEL	DE

APPL-NO: DE00104461

APPL-DATE: November 29, 2001

PRIORITY-DATA: DE00104461W (November 29, 2001)

INT-CL (IPC): H04L009/32 , H04L029/06 , H04Q007/38

EUR-CL (EPC): H04L009/32 , H04L029/06 , H04L029/06 , H04Q007/38

ABSTRACT:

CHG DATE=20030902 STATUS=O>A very efficient authentication and authorisation check in n: m relationships is possible with a method for checking the entitlement of a user of a telecommunication terminal (1) to a service, whereby an access device (4) on a telecommunication network (3) obtains at least one certificate and a proof of identity (10) from the telecommunication terminal (1), whereupon NMT (5) together with a certification device (7) carries out a check of whether the certificate giving the identity is valid and has a positive status and whether particular authorisation may be obtained from complementary certificates. Should the above be the case, a secret (for example a session key) is transmitted (15) to the access device (4) which is also sent (15, 16) to the telecommunication terminal (1, 2), encoded with at least the public key. The access device (4) is then activated with a policy corresponding to the rights of the telecommunication user.